


Havells India

Access Control Policy

Version 1.0

Havells India Limited Havells India Access Control Policy Version 1.0 Internal	 HAVELLS
---	---

Document Control


S. No.	Type of Information	Document Data
1.	Document Title	Havells India Access Control Policy
2.	Document Code	HACP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head (ISH)	ramanand.jha@havells.com

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Havells India Limited Havells India Access Control Policy Version 1.0 Internal	 HAVELLS
---	---

Document Scope

This document shall be applicable to the IT Department and the employees/Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing and managing information/information assets of Havells.

Document Distribution

The Information Security Head (ISH) shall distribute this policy to all employees working with IT department and/or handling, processing and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose5

1.1 Scope5

1.2 Responsibility5

1.3 Enforcement5


1.4 Authority5

1.5 Abbreviations and Definitions:5

2. Policy6

2.1 User Access Management6

2.2 Access Control Audit 10

<p style="text-align: center;">Havells India Limited Havells India Access Control Policy Version 1.0 Internal</p>	
--	---

1. Purpose

This policy intends to establish guidelines for user access creation, modification, deletion, and review of access rights so as to maintain the access controls within Havells and to protect information and information assets against unauthorised access.

1.1 Scope

This policy shall be applicable to the IT department and the employees/Third Party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells including SAP and Non-SAP applications

1.2 Responsibility

It is the responsibility of the IT Team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the Access Control Policy.

1.3 Enforcement

All Employees and/or Third Party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

- a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.
- b) Employees and Third Parties who breach this policy shall be subject to disciplinary action.


Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the *Security Exception Management Policy*.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head (ISH) approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

1.5 Abbreviations and Definitions:

- a) User: User shall include employees of Havells, and Third Party associated/working with /for Havells;
- b) Third Party employees: Third Party is defined as an entity with whom Havells does business. They shall include IT Contractors, vendors, associates , auditors etc.;
- c) Head of Department (HOD): HOD shall be the personnel delegated as the head of a particular department who shall be responsible for approving accesses in certain exceptional cases or as required;
- d) SAP GRC: SAP Governance, Risk and Compliance;
- e) PIM: Privilege Identity Management

<p style="text-align: center;">Havells India Limited Havells India Access Control Policy Version 1.0 Internal</p>	
--	---

2. Policy

Access to Havells' information and information systems shall be controlled in accordance with the relevant business requirement, security policy and processes, and shall be subject to the principles of least privilege and segregation of duty.

2.1 User Access Management


The User access management process shall encompass all stages in the life cycle of user access- from the initial registration to the final de-registration of users, including allocation of and authorisation required for privileged access rights. The process shall include:

- a) Identification of account types (i.e., individual, group, system, etc.) and establishment of conditions for group membership, and assignment of associated authorisations;
- b) Identification of authorised users of the information system (both privilege and standard rights);
- c) Access shall be granted to users based on:
 - i. Approved standard user profile;
 - ii. Need-to-know basis that is determined by assigned official duties, after due approvals from respective functional heads and/ IT Head/ GRC access control approval matrix;
 - iii. Intended system usage
- d) Access creation and modification procedures, including procedures for privilege access request and approval;
- e) Procedures to remove or disable access in case of notification of a change in user status such as when the user:
 - i. Departs from the company;
 - ii. Transfers to another department;
 - iii. Is suspended;
 - iv. Goes on long term leave; or
 - v. Information system usage or need-to-know changes.

2.1.1 Access Creation and Modification

2.1.1.1 Access Creation for Windows ID, Email

- a) **For on-roll new joiners:**
 - i. Based on joining form received from the candidate, HR (Human Resources) team shall validate the documents and shall forward it to the head office payroll accounting team / HR for creation of employee code;
 - ii. After the employee code is generated, the new joiner's email ID/ domain ID is created through an automated system and new joiner is updated/informed through SMS;

<p style="text-align: center;">Havells India Limited Havells India Access Control Policy Version 1.0 Internal</p>	
--	---

b) For third party/associate personnel/consultants:


- i. Vendor code shall be created by the accounts team through a vendor form as per business requirements. Domain ID/ email ID shall be created post approval from HOD, HR and respective IT Lead.

Note: User ID Naming Guidelines

- a) User IDs shall be created in the format of firstname.lastname (e.g. if the name of employee is Raj Malhotra, then user ID created shall be raj.malhotra);
- b) In case if there is a middle name, then the same shall be merged with first name (e.g. If the name of employee is Raj Kumar Malhotra, then user ID created shall be **rajkumar.malhotra**);
Note: In case of windows ID creation, employee ID shall be used. The naming conventions being followed may differ for each of Havells' geography/region.
- c) If required , Creation of Generic IDs because of operational/functional requirements approval from HOD and IT Security Exception shall be obtained before the creation of such IDs and such IDs shall be mapped with the respective owner(s) and tracked for any change;
- d) Information Systems shall not generate any default user IDs that permit unauthenticated system access;
- e) Users shall not approve their own access. Segregation of duties shall exist between the requestor and approver for authorisation;
- f) Assigning of access privileges, including administrator rights, to the user shall only be in accordance with the user's role and after appropriate approval(s) are taken. The access shall only be used for legitimate business purposes and shall be removed when no longer necessary;
- g) All user details shall be traceable to an accountable individual within Havells or any Third Party responsible for operating the system;

2.1.1.2 Non-SAP User Access Creation and Modification

- a) After the employee is on-boarded, his ID shall be created in AD (Active Directory) according to payroll designation band. This grants employee access to O365 services (Outlook, Teams, etc.);
- b) Access to other non-SAP applications shall be given after appropriate approvals from HOD, respective functional head
- c) In case of Third-Party employees /associates, vendor code shall be created in SAP which shall be linked to Active Directory (AD) ID, if created. AD-ID for Third Party employees shall be created after taking approvals from HOD / respective Functional Head, HR, and respective IT Lead. AD ID for Third Party shall be created for a limited time period;
- d) In case of role modification, request should be approved by respective functional head/HOD.

<p style="text-align: center;">Havells India Limited Havells India Access Control Policy Version 1.0 Internal</p>	
--	---

2.1.1.3 SAP User Access Creation and Modification

- a) After creation of User ID by Head Office Payroll accounting team, SAP user ID shall be created automatically for access to SAP ESS (SAP Employee Self Service).
Further, if required, depending on the job key/system authorization maintained in master data, SAP roles are assigned to user through SAP GRC workflow which is approved by respective Functional Head;
- b) In case the requestor is Third-party personnel, Location Head/Commercial Head/Functional Head shall decide for ID creation and subsequently SAP GRC process shall be used for ID creation;
- c) In absence of availability of SAP GRC, IDs can be created after approval from respective functional head and IT Head/CIO;
- d) In certain urgent business requirement/mass request, manual ID creation, lock/unlock, deletion, role assignment, revocation shall be granted after taking approval from Risk Management Team and IT Head;
- e) In case of role modification, request should be approved by respective functional head and risk management team.

2.1.2 Access Deactivation

- a) For on roll employee, separation triggers from E-separation module (excluding death, termination & absconding cases). The email ID, domain ID and SAP ID shall be blocked automatically on the last working day of the employee;
- b) In case of any change in last working day, the location human resource head/ head office-human resource head shall be responsible to update the same on the e-separation module on real time basis;
- c) For excluded cases (such as death, termination & absconding cases), location human resource head must inform head office-human resource head, who shall notify the IT team to manually block the respective IDs;

For off-roll employees/ associates, location human resource head shall inform head office-human resource head, who shall notify the IT team to manually block the IDs

2.1.3 Privilege Management

Privilege access shall be granted after due approval by CIO/ISH (as required). Following section covers privilege access to SAP and Non-SAP Applications.

2.1.3.1 Granting SAP Privileges:


- a) All the SAP privilege access shall be granted through SAP GRC Tool, e.g. during the creation of new privilege request or when a user requests for additional privileges due to changes in job function or changes in responsibilities;

- b) Access approval for SAP_ALL (profile) shall also be managed by SAP GRC tool. It shall require approval from IT Head & Risk management team
- c) SAP_ALL profile may be granted to remote and job users for performing background job scheduling/ running after due approval process;
- d) Privileges shall be allocated to individuals on a 'need-to-have' basis in strict adherence to the authorisation process for privilege access;
- e) Privileged account identifiers that are not uniquely assigned to an individual for their exclusive use and that are necessary to configure and operate an Information System (e.g., shared accounts, service accounts, enterprise administrator accounts, and all other privileged accounts etc.) shall be identified and documented;
- f) All service accounts shall be assigned to a responsible individual for use, and protection of the authentic credentials associated with a particular service account.

2.1.3.2 Non-SAP & Infrastructure Privilege Management:

- a) For non-SAP applications IT department should identify all the privileges allocated to users within Havells environment;
- b) PIM / TACAS Tool shall be used for delegating the privilege accounts such as root/enterprise/network admin access after appropriate approvals on a need-to-use basis and on an event-by-event basis;
- c) IT shall ensure access to critical systems via PIM (Privilege Identity Management) / TACAS only, wherever applicable. Any exception to be approved by CIO and Information Security Head (ISH) (as required);
- d) PIM / TACAS Administrator shall issue privilege password after receiving a request from IT team with the approval from CIO / ISH;
- e) After the completion of task using these privileges, PIM / TACAS Administrator shall change the password immediately in the PIM / TACAS tool, if the password was handed over to IT admin.

	Normal/Read Access	Admin privileged Access Approvals	Access to Functional Team
Infra Access	NA	CIO/Information Security Head and Functional Head	Default access will be given to the users based on their job profile
Application & DB	Reporting Manager/Application Owner/D&E Head		
EDW(Dashboard) Application & DB	Application Owner		

Havells India Limited Havells India Access Control Policy Version 1.0 Internal	 HAVELLS
---	---

IT System	Access Type	ID/Account Type	Role
Operating System	Administrator	RW	Production Support Team (L1/L2/L3 Support)/Application Vendor (To manage their App and DB)
	Read Access	RO	NA
Data Base	Administrator/Super User/Service Account/Application User/DB Owner	RW	Production Support Team (L1/L2/L3 Support) /D&E Team/Application Vendor (To manage their App and DB)
	View/Read access	RO	D&E Team on approval of D&E head/Application Owner/Application Vendor (To manage their App and DB)

2.1.4 Segregation of Duties

- While enabling user access in applications, roles to be assigned in such a manner that it eliminates conflict of interest in the responsibilities and duties of individuals;
- Periodic review to be conducted at least once a year to avoid any conflict. Such review shall be jointly performed by respective function and IT Team.

2.1.5 Review of User Access Rights

- For privilege users, access review shall be performed on an annual basis;
- For non-privilege users, access to critical applications such as SAP shall be performed on an annual basis;
- Whenever there is a change in the role of a user or a transfer from one function / geography to another function / geography, access rights shall be revoked and reassigned on a “need-to-know” basis.

2.2 Access Control Audit

Audit trail shall be enabled for privilege access users to the extent practicable. Such audit logs shall be periodically reviewed.